

DII.3200.HP1020.SMG-1

Defense Information Infrastructure (DII)

Common Operating Environment (COE)

Version 3.2.0.0

Security Manager's Guide (HP-UX 10.20)

July 25, 1997

Prepared for:

Defense Information Systems Agency

Prepared by:

**Inter-National Research Institute (INRI)
12200 Sunrise Valley Drive, Suite 300
Reston, Virginia 20191**

Table of Contents

Preface	1
1. Introduction	3
1.1 Overview	3
1.2 Referenced Documents	4
2. Security Administration Login and Overview	5
3. Assigning Passwords	7
4. Modifying Profiles	11
5. Unlocking Users	15
6. Changing the secman Password	19

List of Figures

Figure 1. DII COE Login Screen	5
Figure 2. Assign Passwords Window Sorted by User Name	7
Figure 3. Assign Passwords Window Sorted by User ID	8
Figure 4. Set Password Window	8
Figure 5. Verify Password Window	9
Figure 6. USER PROFILES Window	11
Figure 7. EDIT PROFILE Window	12
Figure 8. EDIT PERMISSIONS Window	13
Figure 9. EDIT MENU ACCESS Window	14
Figure 10. User Account Information Window	16
Figure 11. User Account Information Window with User Account Information	17
Figure 12. Set Password Window	19
Figure 13. New Password Window	20

This page intentionally left blank.

Preface

The following conventions have been used in this document:

[HELVETICA FONT]	Used to indicate keys to be pressed. For example, press [RETURN].
Courier Font	Used to indicate entries to be typed at the keyboard, operating system commands, titles of windows and dialog boxes, and screen text. For example, execute the following command: <pre>tar xvf /dev/rmt/3mn</pre>
<i>Italics</i>	Used for emphasis.

This page intentionally left blank.

1. Introduction

1.1 Overview

This document provides general information about the Defense Information Infrastructure (DII) Common Operating Environment (COE) and the security administration capabilities of the DII COE kernel. See the *DII COE Integration and Runtime Specification* for more information about the DII COE. See the *DII COE Kernel Installation Guide (HP-UX 10.20)* for more information about installing the DII COE kernel and segments.

This guide is divided into the following sections:

Section	Page
Security Administration Login and Overview Describes how to access DII COE Security Administration functionality.	5
Assigning Passwords Describes how to assign a password to an existing local or network user.	7
Modifying Profiles Describes how to modify profiles to add and restrict access to functions within menus and options using the <code>Edit Profiles</code> icon.	11
Unlocking Users Describes how to unlock a user who has been locked out of the system.	15
Changing the <code>secman</code> Password Describes how to change the <code>secman</code> password.	19

1.2 Referenced Documents

The following documents are referenced in this guide:

- C DII COE I&RTS:Rev 3.0, *Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification* Version 3.0, January 1997
- C DII.3200.HP1020.Kernel.IG-1, *Defense Information Infrastructure (DII) Common Operating Environment (COE) Version 3.2.0.0 Kernel Installation Guide (HP-UX 10.20)*, July 25, 1997
- C DII.3200.HP1020.AG-1, *Defense Information Infrastructure (DII) Common Operating Environment (COE) Version 3.2.0.0 System Administrator's Guide (HP-UX 10.20)*, July 25, 1997
- C JPL D-13867, Release 2, *Defense Information Structure (DII) Security Manager Administrator's Guide DRAFT*, June 15, 1997.

2. Security Administration Login and Overview

To access DII COE Security Administration functionality, you must enter the `secman` login name and the `secman` password. Only user accounts that are assigned to profiles under the Security Admin account group may run Security Manager. The `DII COE Login` screen (Figure 1) and the DISA security screen appear any time a machine loaded with the HP-UX 10.20 Operating System and the DII COE kernel is rebooted or any time a user logs out of the system at the console.

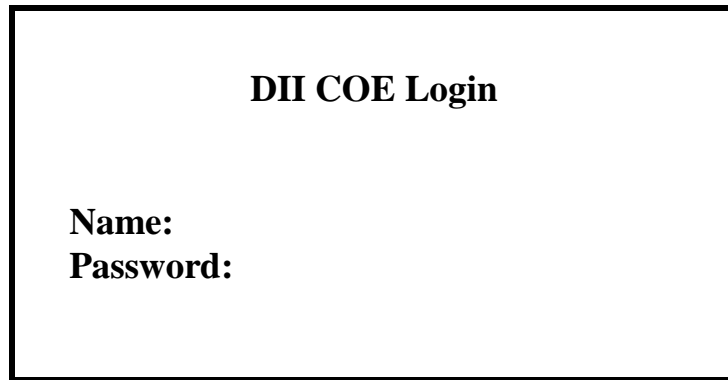
A rectangular window with a black border. At the top center, the text "DII COE Login" is displayed in a bold, black, sans-serif font. Below this, on the left side, are two labels: "Name:" and "Password:", each followed by a blank space for input. The text is in a bold, black, sans-serif font.

Figure 1. DII COE Login Screen

Follow the steps below to log in with a `secman` account and access DII COE Security Administration functionality.

- STEP 1: **Log in as the security manager.** Type `secman` at the Name prompt in the `DII COE Login` window (Figure 1) and press [RETURN].
- STEP 2: **Enter the `secman` password.** Type the `secman` password at the Password prompt in the `DII COE Login` window (Figure 1) and press [RETURN]. The Security Management software appears.
- STEP 3: **Access the Application Manager.** Double-click on Application Manager on the Common Desktop Environment (CDE) panel. The Application Manager window appears. See Section 5 of the *DII COE System Administrator's Guide (HP-UX 10.20)* for more information about CDE.
- STEP 4: **Select the `DII_APPS` folder.** Double-click on the `DII_APPS` folder. The Application Manager - `DII_APPS` window appears.
- STEP 5: **Select the `SSO_Default` folder.** Double-click on the `SSO_Default` folder. The Application Manager - `SSO_Default` window appears.

The Application Manager - SSO_Default window contains the following security management icons:

- C Assign Passwords
- C Edit Profiles
- C Profile Selector Config
- C Security Manager
- C Security Mgr Remote
- C Unlock Users
- C Update Security DB.

The Profile Selector Config, Security Manager, Security Mgr Remote, and Update Security DB icons and their associated functionality are described in the *DII Security Manager Administrator's Guide*. See the *DII Security Manager Administrator's Guide* for information about accounts and profiles, the Security Manager application and system configuration, and profile directives, as well as information about running Security Manager. The Assign Passwords, Edit Profiles, and Unlock Users icons are described in the following subsections.

In addition to describing the icons above, this guide describes the Chg Password icon. To access this icon, select the DII_TOOLS folder from the Application Manager window. The Application Manager - DII_TOOLS window appears. The Application Manager - DII_TOOLS window contains the Chg Password icon.

3. Assigning Passwords

Passwords can be changed for existing local or network user accounts using the Assign Password icon. Follow the steps below to assign passwords to existing user accounts.

- STEP 1: Log in as the security manager.** Type `secman` at the Name prompt in the DII COE Login window (Figure 1) and press [RETURN].
- STEP 2: Enter the `secman` password.** Type the `secman` password at the Password prompt in the DII COE Login window (Figure 1) and press [RETURN]. The Security Management software appears.
- STEP 3: Access the Application Manager.** Double-click on Application Manager on the CDE panel. The Application Manager window appears. See Section 5 of the *DII COE System Administrator's Guide (HP-UX 10.20)* for more information about CDE.
- STEP 4: Select the `DII_APPS` folder.** Double-click on the `DII_APPS` folder. The Application Manager - `DII_APPS` window appears.
- STEP 5: Select the `SSO_Default` folder.** Double-click on the `SSO_Default` folder. The Application Manager - `SSO_Default` window appears.
- STEP 6: Select the Assign Passwords icon.** Double-click on the Assign Passwords icon to open the Assign Passwords window (Figure 2). The window shown in Figure 2 contains a list of local user accounts sorted by user name because the User Name toggle has been selected in the Sort by panel.

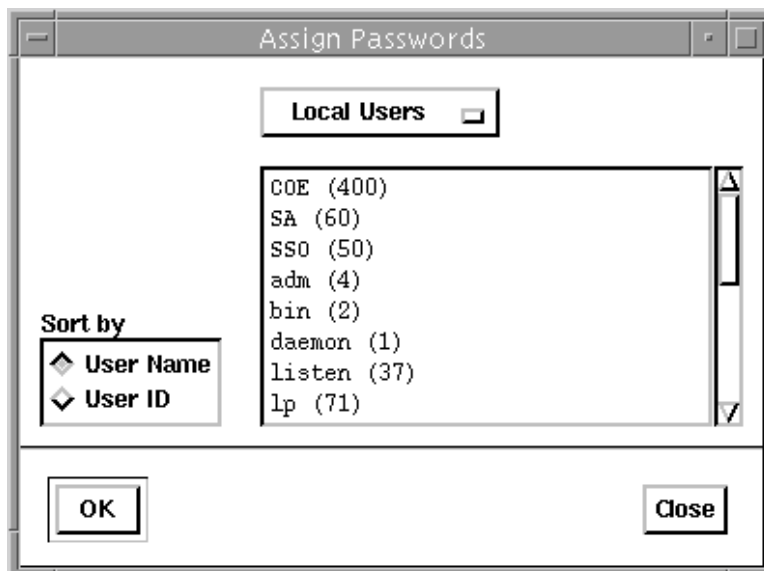


Figure 2. Assign Passwords Window (Sorted by User Name)

Figure 3 contains a list of local user accounts sorted by user ID because the `User ID` toggle has been selected in the `Sort by` panel.

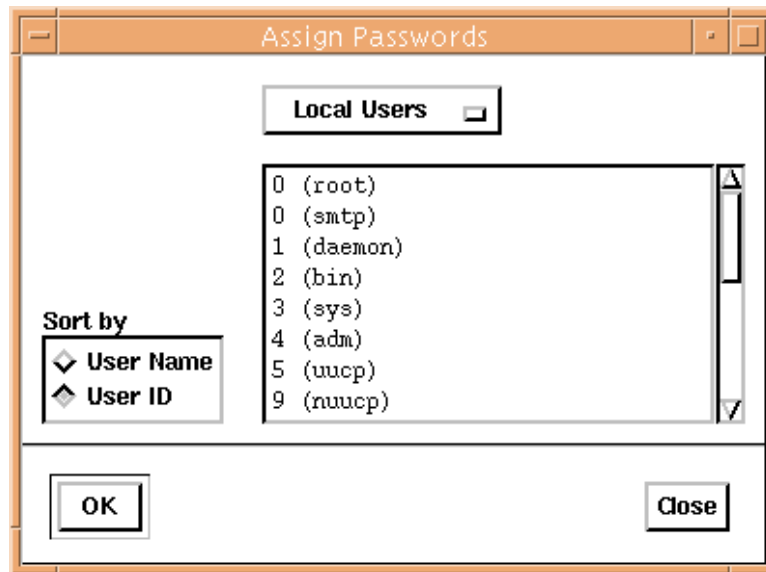


Figure 3. Assign Password Window Sorted by User ID

- STEP 7: **Determine if you want to view a list of local user accounts or network user accounts.** Click on the button at the top of the window to select either the `Local Users` option or the `Network Users` option.
- STEP 8: **Determine if you want to view the list of user accounts by user name or by user ID.** Click on the `User Name` toggle or the `User ID` toggle in the `Sort by` panel.
- STEP 9: **Select the user account for whom you want to assign a password.** Click on a user account to highlight it and then click on the `OK` button. The `Set Password` window appears (Figure 4).

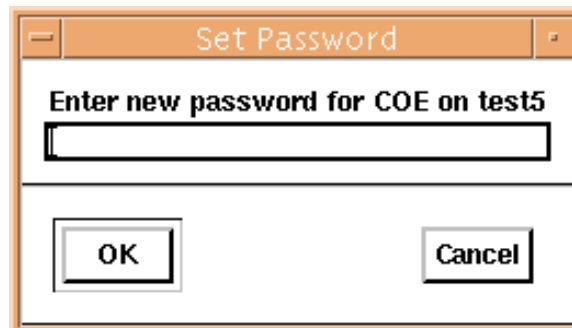


Figure 4. Set Password Window

STEP 10: **Enter a new password.** Type a new password in the Enter new password for [user name] on [machine name] field and click on the OK button. The Verify Password window appears (Figure 5).



Figure 5. Verify Password Window

STEP 11: **Re-enter the password.** Retype the password in the Verify New Password field and click on the OK button.

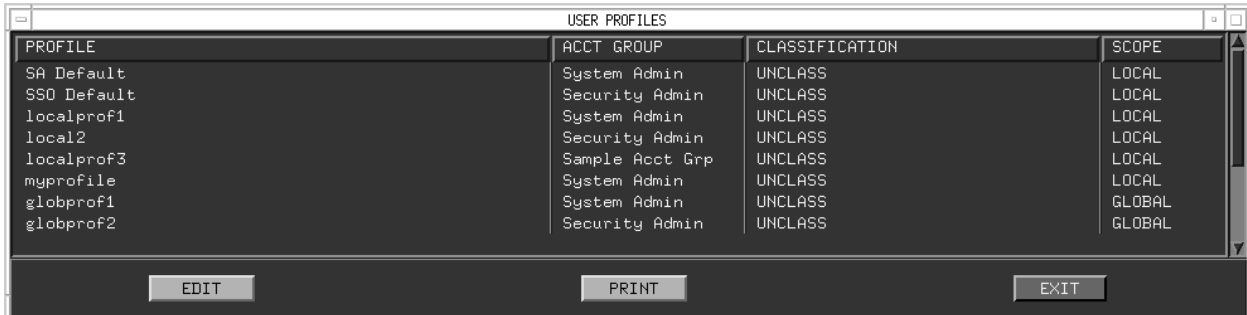
STEP 12: **Assign a password for other user accounts or exit the Assign Password window.** Assign a password for other user accounts by following STEPS 7-11 for each user account. When you are done assigning passwords to user accounts, click on the Close button to exit the Assign Password window (Figure 2).

This page intentionally left blank.

4. Modifying Profiles

Once created and defined, you can modify profiles to add and restrict access to functions within menus and options using the `Edit Profiles` icon. Follow the steps below to modify profiles.

- STEP 1: Log in as the security manager.** Type `secman` at the `Name` prompt in the `DII COE Login` window (Figure 1) and press `[RETURN]`.
- STEP 2: Enter the `secman` password.** Type the `secman` password at the `Password` prompt in the `DII COE Login` window (Figure 1) and press `[RETURN]`. The Security Management software appears.
- STEP 3: Access the Application Manager.** Double-click on `Application Manager` on the `CDE` panel. The `Application Manager` window appears. See Section 5 of the *DII COE System Administrator's Guide (HP-UX 10.20)* for more information about `CDE`.
- STEP 4: Select the `DII_APPS` folder.** Double-click on the `DII_APPS` folder. The `Application Manager - DII_APPS` window appears.
- STEP 5: Select the `SSO_Default` folder.** Double-click on the `SSO_Default` folder. The `Application Manager - SSO_Default` window appears.
- STEP 6: Select the `Edit Profiles` icon.** Double-click on the `Edit Profiles` icon to open the `USER PROFILES` window (Figure 6). The `USER PROFILES` window lists all user profiles you can modify.



PROFILE	ACCT GROUP	CLASSIFICATION	SCOPE
SA Default	System Admin	UNCLASS	LOCAL
SSO Default	Security Admin	UNCLASS	LOCAL
localprof1	System Admin	UNCLASS	LOCAL
local2	Security Admin	UNCLASS	LOCAL
localprof3	Sample Acct Grp	UNCLASS	LOCAL
myprofile	System Admin	UNCLASS	LOCAL
globprof1	System Admin	UNCLASS	GLOBAL
globprof2	Security Admin	UNCLASS	GLOBAL

EDIT PRINT EXIT

Figure 6. `USER PROFILES` Window

- STEP 7: Select a profile to modify.** To modify a profile's access to functions within menus and options, click on the profile to select it and click on the `EDIT` button.

NOTE: `SA_Default` and `SSO_Default` user profiles cannot be edited. If you select one of these, the `CANNOT MODIFY` warning window appears. Click on the `OK` button to close it.

STEP 8: Review the information in the EDIT PROFILE window. The EDIT PROFILE window appears (Figure 7). The PERMISSIONS panel shows the applications that have been assigned to that profile.

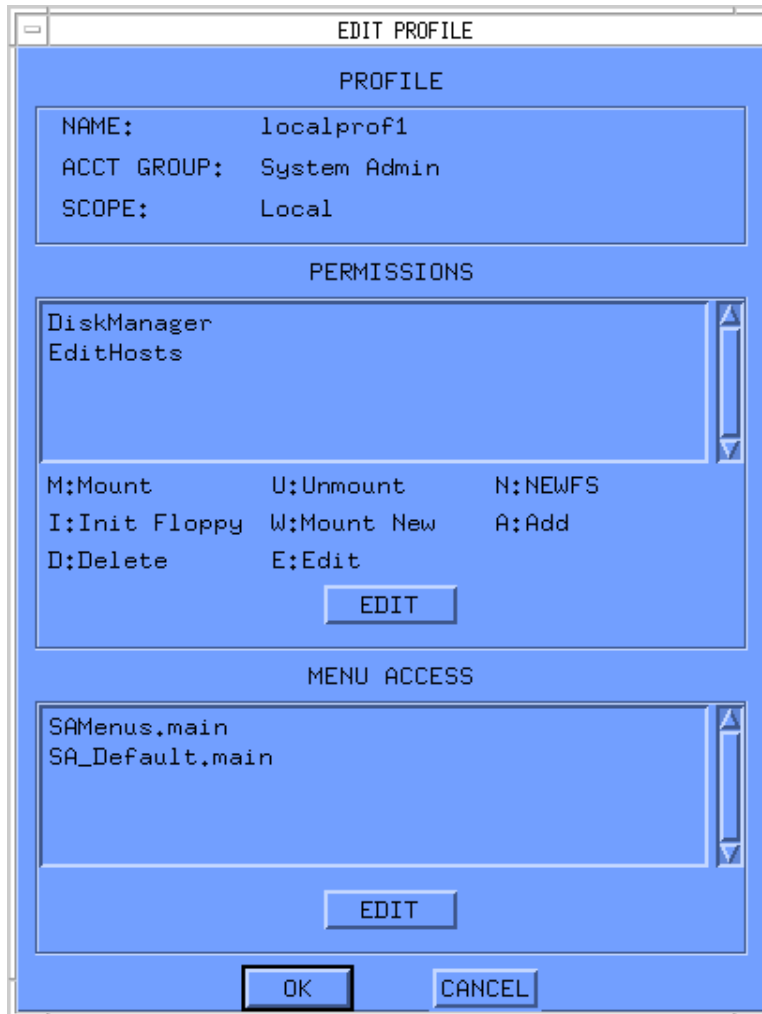


Figure 7. EDIT PROFILE Window

STEP 9: Modify permissions, if desired. Highlight an option in the PERMISSIONS panel and click on the EDIT button to modify permission settings for the option. For example, in the EDIT PROFILE window (Figure 7), click on a permission such as the DiskManager option and click on the EDIT button.

STEP 10: Set permissions for the option. The EDIT PERMISSIONS window appears (Figure 8). Figure 8 shows DISKMANAGER PERMISSIONS because the DiskManager option was selected in STEP 8. Click on the options for which the profile should have permissions. For example, if you want the profile to be able to mount a file system and unmount a file system, you would click on the Mount and Unmount toggles in Figure 8. Click on the OK button when you finish selecting options. The EDIT PROFILE window (Figure 7) returns to the forefront.

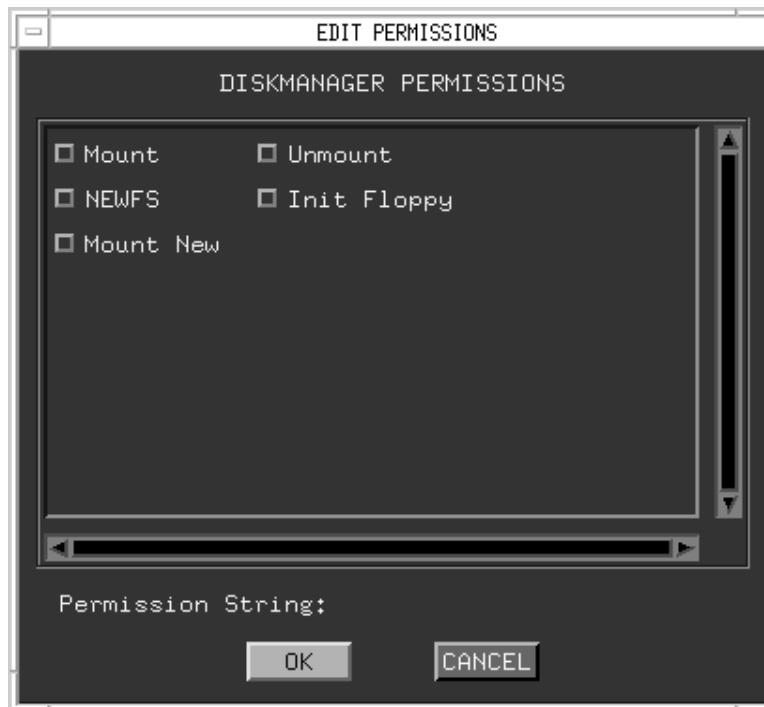


Figure 8. EDIT PERMISSIONS Window

STEP 11: Modify menu access, if desired. Highlight a menu in the MENU ACCESS panel and click on the EDIT button to modify menu access settings for the option. For example, in the EDIT PROFILE window (Figure 7), click on a menu access option such as the SAMenus.main option and click on the EDIT button.

STEP 12: Set menu access settings. The `EDIT MENU ACCESS` window appears (Figure 9). Figure 9 shows System Administration menus because the `SAMenus.main` option was selected in STEP 10. Click on the menus for which the profile should have permissions. For example, if you want the profile to have access to the Help menu and the SA System menu, you would click on the Help and SA System toggles in Figure 9. Click on the OK button when you finish selecting options. The `EDIT PROFILE` window (Figure 7) returns to the forefront.

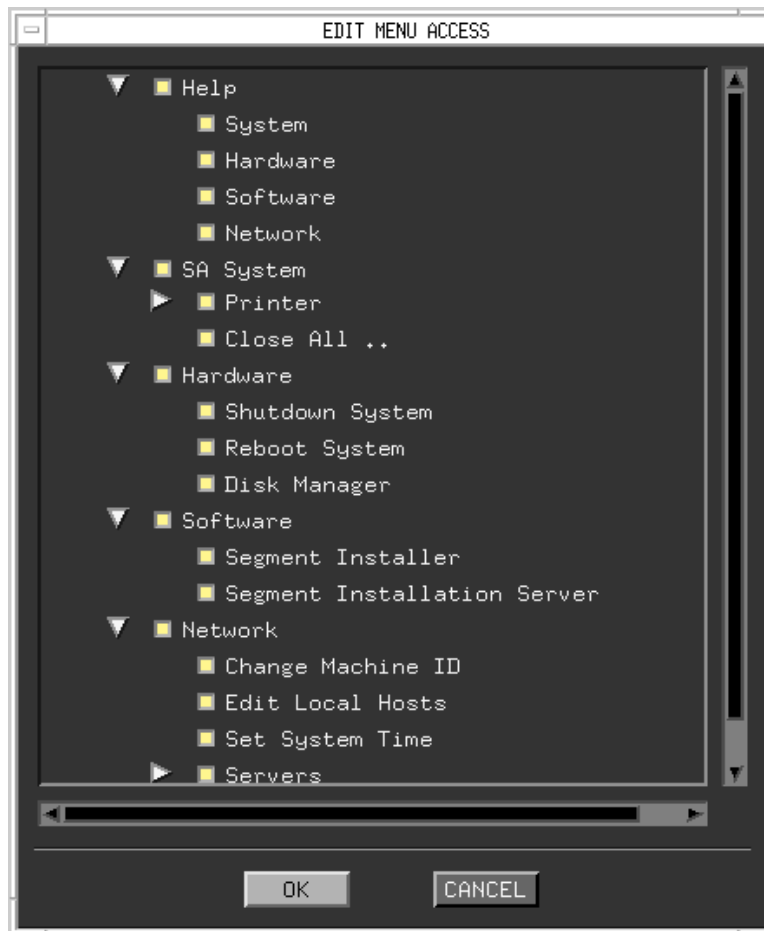


Figure 9. EDIT MENU ACCESS Window

STEP 13: Apply your changes. Click on the OK button in the `EDIT PROFILE` window (Figure 7) to apply your changes and exit the window.

5. Unlocking Users

A user account is disabled automatically the third consecutive time an incorrect password is entered for that account. When an account is disabled, a message similar to the following appears:

```
Account is disabled -- see Account Administrator.
```

Disabled user accounts can be unlocked using the `Unlock Users` icon. Follow the steps below to re-enable a user account that has been disabled.

- STEP 1: **Log in as the security manager.** Type `secman` at the `Name` prompt in the `DII COE Login` window (Figure 1) and press `[RETURN]`.
- STEP 2: **Enter the `secman` password.** Type the `secman` password at the `Password` prompt in the `DII COE Login` window (Figure 1) and press `[RETURN]`. The Security Management software appears.
- STEP 3: **Access the Application Manager.** Double-click on `Application Manager` on the CDE panel. The `Application Manager` window appears. See Section 5 of the *DII COE System Administrator's Guide (HP-UX 10.20)* for more information about CDE.
- STEP 4: **Select the `DII_APPS` folder.** Double-click on the `DII_APPS` folder. The `Application Manager - DII_APPS` window appears.
- STEP 5: **Select the `SSO_Default` folder.** Double-click on the `SSO_Default` folder. The `Application Manager - SSO_Default` window appears.

STEP 6: Select the unlock users icon. Double-click on the Unlock Users icon to open the User Account Information window (Figure 10).

The screenshot shows the 'User Account Information' window. The 'Users' tab is selected. The 'Host' list box contains the following items: boss, garcia, hp1010, jasmine, localhost. The 'User' list box is empty. The 'Results' section is empty. The right-hand form contains the following fields:

- User Name: [] User ID: [] Group ID: []
- Account Access: []
- Full Name: []
- Office: []
- Office Phone: [] Home Phone: []
- Organization: []
- Social Security Number: [] Rank: []
- Home Directory: []
- Login Shell: [] File Server: []
- Login Failures: [] Last Login Failure: []
- Groups: []
- Last Login: []

Figure 10. User Account Information Window

STEP 7: Select the host machine for which a user has been locked out. Click on a host machine for which a user has been locked out in the Host panel to select it, and then select the Update for Selected Host option from the Users pull-down menu. All valid user accounts for the selected machine appear in the User panel by default.

NOTE: If you want to select the host machine you are currently using, select localhost.

STEP 8: Determine if you want to view all user accounts or a subset of all user accounts. If you want to view all user accounts, proceed to STEP 9. If you want to tailor the list of user accounts to view particular users, select the Local Users option, Network Users option, Logged In Users option, Enabled Users option, Disabled Users option, Locked Out Users option, or Users with Failed Logins option from the View pull-down menu. In the User panel, the letter L beside a user account indicates a locked account; the letter F beside a user account indicates an account with one or two login failures; and the letter I beside a user account name indicates the user account with which you logged in to the machine.

NOTE: If you just want to view a list of locked out users, select the Locked Out Users option. If you want to view a list of all user accounts with at least one login failure (including locked out users), select the Users with Failed Logins option.

STEP 9: Select the user account that has been locked out of the selected host machine. Click on a user account in the User panel; the letter L should appear beside this user account. Information about that user account appears in the panel on the right side of the User Account Information window, as shown in Figure 11.

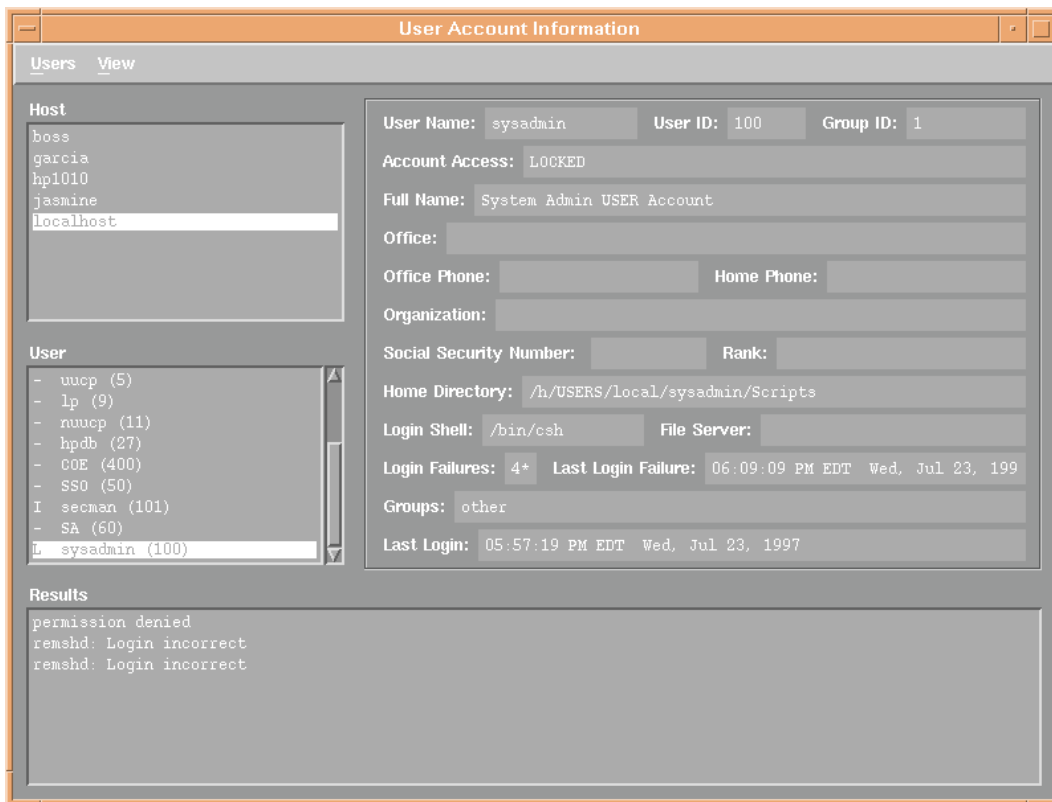


Figure 11. User Account Information Window with User Account Information

For example, in Figure 11, the `Account Access` field shows that the user account is `LOCKED`, the `Login Failures` field shows that more than three (4+) login failures have occurred, and the `Last Login Failure` field shows the date and time of the last login failure.

STEP 10: Clear the selected user's login failures. Select the `Clear Login Failures` option from the `Users` pull-down menu. In the `User` panel, the letter `L` no longer appears beside the cleared user account.

NOTE: If any commands do not work as expected, one or more messages appear in the `Results` panel of the window.

STEP 11: Update information about the cleared user account. To ensure that the user account is cleared, click on the user account in the `User` panel. The `Account Access` field in the panel on the right side of the `User Account Information` window updates to show that the user account is `ENABLED`.

STEP 12: Exit the User Account Information window. Select the `Exit` option from the `Users` pull-down menu to exit the `User Account Information` window.

6. Changing the secman Password

Follow the steps below to change the secman password.

- STEP 1: **Log in as secman.** Type secman at the Name prompt and press [RETURN].
- STEP 2: **Enter the secman password.** Type the secman password at the Password prompt and press [RETURN]. The Security Management software appears.
- STEP 3: **Access the Application Manager.** Double-click on the Application Manager control on the CDE Front Panel to open the Application Manager window.
- STEP 4: **Select the DII_TOOLS folder.** Double-click on the DII_TOOLS folder in the Application Manager window to open the Application Manager - DII_TOOLS folder.
- STEP 5: **Select the chg Password icon.** Double-click on the Chg Password icon to open the Set Password window (Figure 12).

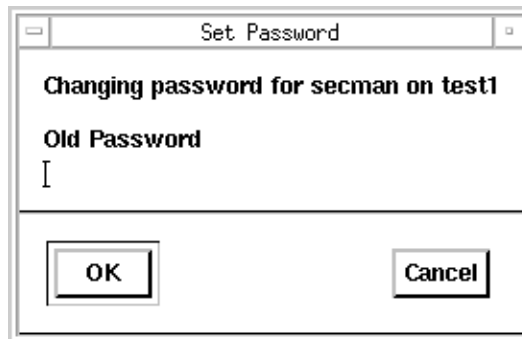


Figure 12. Set Password Window

- STEP 6: **Enter the current secman password.** Enter the current secman password in the Old Password field and click on the OK button.

STEP 7: Enter the new secman password. The New Password window appears (Figure 13). Enter the new secman password in the Enter New Password field and click on the OK button.



Figure 13. New Password Window

STEP 8: Verify the new secman password. The Verify New Password window appears. Enter the new secman password in the field and click on the OK button.

STEP 9: Acknowledge that the secman password has changed. Click on the OK button when the following message appears:

Your password has been successfully updated!